16th Annual Government Financial Management Conference

Public/Private Identity Authentication: A Progress Report

August 8, 2006 -- 1:30 p.m. -- Ronald Reagan Building

Georgia K. Marsh
Deputy Program Manager
General Service Administration
eAuthentication Federation

Jim Gross
Senior Vice President
Wells Fargo
WellsSecure

In A Nutshell . . .

"All truth passes through three stages.

First, it is ridiculed.

Second, it is violently opposed.

Third, it is accepted as being self-evident."

--Arthur Schopenhauer (1788-1860)

We pleased to report that
public/private authentication services
are moving very close to Schopenhauer's third stage

Agenda

- E-Authentication Federation Status Update
- Private Sector Status Update
  - Federation Makes The Opportunities
  - Federal Agencies Drive The Opportunities
- The Challenges Still Ahead

E-Authentication Federation Status Update

A Federation is Born

Certificate of Birth

The E-Authentication Federation

Born on:

October 18, 2005

The Goal of E-Government

Empower and enable citizens and businesses to manage their relationships with government on their terms in a *secure online environment*

The Role of the E-Authentication Program

Provide standards, framework and services necessary for the Federal Government to accept all levels of secure identity verification, simplifying business, public & government access to online services in a cost-effective manner

E-Authentication Mission

- Enable millions of safe, secure, trusted online transactions between Government and the citizens and businesses that it serves
- Reduce online identity management / credentialing burden for government agency application owners and system administrators
- Provide citizens and businesses with a choice of credentials – such as PINs / User IDs / passwords / digital certificates – when accessing public-facing online government services

Key Policy Considerations

- For Government-wide deployment:
  - No National ID
  - No National unique identifier
  - No central registry of personal information, attributes, or authorization privileges
  - Different authentication assurance levels are needed for different types of transactions
  - Authentication – not authorization
- For E-Authentication technical approach:
  - No single proprietary solution
  - Deploy multiple COTS products – user's choice
  - Products must interoperate
  - Controls must protect privacy of personal information

E-Authentication Strategy

- The best way to accomplish E-Authentication's mission while satisfying the requisite policy considerations:
  - Build the ***E-Authentication Federation***, wherein government agencies can rely on electronic identity credentials issued and managed by other organizations within and **outside the federal government**

The Concept of E-Authentication

Step 1:

At access point (agency Web site or credential service provider) user selects agency application and credential provider

Step 2:

- User is redirected to selected credential service provider
- If user already possesses credential, user authenticates
- If not, user acquires credential and then authenticates

Step 3:

- User performs transaction
- Credential service hands off authenticated user to the agency application selected

The Building Blocks of the E-Authentication Federation

Agency Applications/
Credential Service Providers

Growing in FY06 and beyond

Business & Operating Rules

Operational Infrastructure

Completed FY '05

Policy

Technology/Architecture

Completed FY 2004

Finding Credential Service Providers (CSPs)

- The Federal Government does not want to be in the credential management business
- Various commercial entities – insurers and other financial institutions – are natural trusted identity credential providers
- **WHO PROVIDES AUTHENTICATION TODAY?** Look in your wallet – what credentials are you most likely to find?
  - **A bank card**
  - **A health insurance card**
  - **School ID**
  - **A State Government-issued driver's license or photo ID**

Citizen/business convenience and trust are key to selecting credential service providers

Why Financial Institutions

- Authentication lies at the core of existing financial services products
  - Know-your-customer (KYC) required by law
- Financial institutions own 3 powerful assets:
  - Trust
  - 90+% of the US population has banking relationship
  - 53M have bank-issued credentials (Pew)
  - Strongly authenticated identities
- Law requires more than KYC – it requires that customers' identities be protected

E-Authentication's Work with FIs To Date

- Conducted productive pilot with Financial Services Technology Consortium (FSTC)
- Coordinated with Dept. of Treasury's Financial Management Service to leverage "Designation of Financial Agent" authority
  - Means of acquiring authentication services from commercial financial institutions
- Fidelity Investments and Wells Fargo (WellsSecure PKI) have joined the E-Authentication Federation

Immediate Opportunity

- E-Authentication plans to release a **Request for Information (RFI)** this Summer to ascertain the marketplace for providing standards-compliant identity credential services to support the E-Government activities of the Federal Government
- E-Authentication expects to release an RFP for such services by early Fall
- Goal is to have provider or providers in place, supporting the Federation, by this November

The E-Authentication Commercial Value Proposition

- A significant business opportunity for Credential Services Providers
  - Business modeling underway – to find the right model for acquiring such services
- Unique customer service offering
  - Business differentiator
- Increased brand loyalty
  - “Stickiness”

Status of Federation Membership (8/1/06)

Operational* Relying Parties

- **SSA (Direct Deposit)**
- **GSA (eOffer)**
- **Dept. of Labor (MSHA)**
- **OPM (USA Learning)**
- **NASA (MyNASA)**
- **Dept. of Transportation (SAFER)**
- **Dept. of Justice/ATF (BATS)**
- **Dept. of Commerce (Export.gov)**
- **State Dept. (DTAS)**
- **NSF (Fastlane)**
- **Dept. of Energy (VIPERS)**
- **Dept. of Interior (National Park Service)**
- **Dept. of Education (e Payments)**

Credential Service Providers

- **Fidelity Investments***
- **WellsSecure* (Wells Fargo PKI)**
- **ORC**
- **USDA eAuthentication**
- **OPM Employee Express**

* Denotes designated financial agent (DFA) of the US Department of Treasury / Financial Management Service

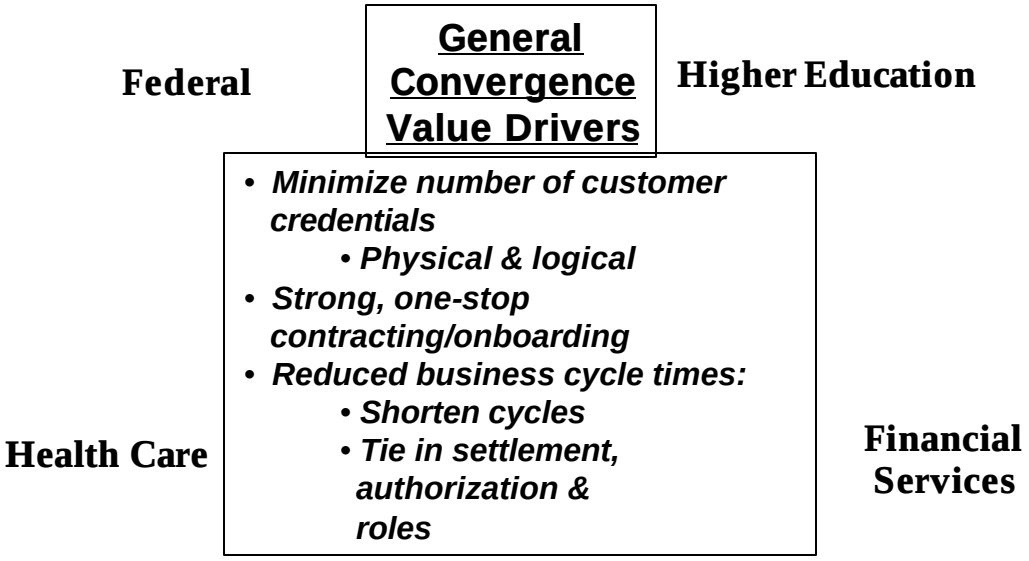
*Applications are currently deployed

Private Sector Status Update

Smart Providers Want What Their Customers Want

- **Identity trust and simplicity count**
- **Federated Identity can help make this real**

Example Federated Trust Communities:



And Outside Forces Are At Work

- The 9/11 effect
- The Katrina effect
- Data breaches
- Application security breaches
- Perceived spoofing and pharming increases

Federated Identity Matures

- Generation I
  - Technical interoperation (logical only)
  - Few enabled applications
  - Lots of “out of band” paper and wet signatures
  - AYOR for the most part -- mostly low assurance
- Generation II
  - Common rules and policies are developed
    - Technology and business processes both interoperate
    - Governance becomes important
    - Higher assurance possible due to lower repudiation risk
  - Increasing scale leads to more applications
  - Digital signatures become more feasible / important
  - Physical access becomes important (in addition to logical)

Federal Agencies Are Driving The Opportunities

For The Private Sector, The Question Is When . . . *Not If*

We believe that [federal] investments made in government identity solutions are already catalyzing the commercial market for these [identity management] technologies.

-- *Stanford Group Company*
July, 2006

- The success of the E-Authentication Federation in signing and implementing private sector identity services contracts is a major milestone in motivating private sector investment and activity
- The upcoming E-Authentication RFI/RFP further increases this motivation

This Is Compounded By HSPD-12 Demand

- Many of the logical identity components supporting E-Authentication are relevant to HSPD-12
- HSPD-12 has driven NIST to establish long awaited technology standards
- Together, E-Authentication and HSPD-12 generate an unprecedented swell of private sector demand and improved federal credibility

Challenges Still Ahead

- Synchronizing demand with supply
  - Identity services provision is not a mature “dial tone” market
  - Buyers expect production readiness -- suppliers cannot afford long stretches of under utilized assets
- Resources / funding for marketing are in short supply
  - Can we make identity services the next “ring tone” must-have market?
- Symbolic compliance purchases

In Summary . . .

- The last year has seen enormous progress in building identity services public / private partnerships
  - Live, federated identity deployments are under way via E-Authentication auspices
  - Increasing interoperability makes the “federal necklace” an endangered specie
- Increasing commercial credibility will improve private sector services availability
- Improving federal government best practices will result in more availability, choice and pricing

Questions? Comments?

Thank You For Your Time Today!

Contact Information

Georgia K. Marsh
Deputy Program Manager
General Service Administration
eAuthentication Federation
2011 Crystal City Drive
Suite 911
Alexandria, VA 22202
V: (703) 872-8614
F: (703) 872-8598
georgiak.marsh@gsa.gov

Jim Gross
Senior Vice President
Wells Fargo
One Front Street, MAC A0195-204
20th Floor
San Francisco, CA 94111
V: (415) 222-5007
F: (415) 788-3039
jgross@wellsfargo.com